. of

-g-slative Audit Division

State of Montana

Report to the Legislature

July 1997

EDP Audit

Adult Correctional Information System

Department of Corrections

This report provides information regarding general and application controls related to the Adult Correctional Information System application. It contains recommendations for improving controls within the department's electronic data processing environment. These recommendations address improving:

- **Data integrity and report accuracy.**
- **Electronic access controls.**
- **Documentation of formal contingency procedures.**

Direct comments/inquiries to:
Legislative Audit Division
Room 135, State Capitol
PO Box 201705
Helena MT 59620-1705

97DP-07

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Legislative Audit Division are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Linda Nelson, Chairman
Senator Sue Bartlett
Senator Reiny Jabs
Senator Tom Keating
Senator Ken Miller
Senator Fred VanValkenburg

Representative Bruce Simon, Vice Chairman
Representative Ernest Bergsagel
Representative Beverly Barnhart
Representative A. R. "Toni" Hagener
Representative Bob Keenan
Representative Robert Pavlovich

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel
Tori Hunthausen, IT & Operations Manager

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
James Gillett, Financial-Compliance Audit

July 1997

The Legislative Audit Committee
of the Montana State Legislature:

This is a report of our EDP audit (97DP-07) of Department of Correction's internal controls relating to its computer-based Adult Correctional Information System (ACIS). We reviewed the department's general controls related to the microcomputer environment which processes ACIS. In addition, we reviewed the ACIS application. This report addresses the control weaknesses we identified in the Department of Correction's EDP system. The department's written response to our audit recommendations is included in the back of the report.

At the request of the Legislative Audit Committee chairman, portions of this report were released to the audit committee and the select committee on corrections, during the 1997 legislative session.

We thank the director and his staff for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Room 135, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@mt.gov

Legislative Audit Division

EDP Audit

Adult Correctional Information System

Department of Corrections

Members of the audit staff involved in this audit were Ken Erdahl, Rene Silverthorne, and Lon Whitaker.

Table of Contents

Table of Contents

List of Figures

Appointed and Administrative Officials

Administrative Services

Rick Day, Director

Sally Johnson, Administrator, Professional Services Division

Bill Furois, Administrator, Management Services Division

Board of Pardons

		Term Expires
Patrick Fleming	Chairman	1/1/99
Gary Weer	Member	1/1/01
Maureen Niehart	Member	1/1/02
Roxanna Wilson	Auxiliary Member	1/1/01
Mark Fournier	Auxiliary Member	1/1/03
Craig Thomas	Executive Director	
Jeff Walter	Administrative Officer	

Community Corrections

Mike Ferriter, Administrator

Mary Fay, Chief, Probation & Parole Bureau

Jim Bauch, Superintendent, Montana Youth Alternatives

Dan Maloughney, Superintendent, Swan River Correctional Treatment Center

John Paradis, Juvenile Placement

Secure Care Facilities

Mike Mahony, Warden, Montana State Prison

Jo Acton, Warden, Women's Correctional Center

Steve Gibson, Superintendent, Pine Hills School

Montana Correctional Enterprises

Ron Paige, Ranch Manager

Glen Davis, Industries Manager

Dave Watkins, Vocational Education Manager

Ross Swanson, Business Manager

Introduction

The Department of Corrections (DOC) uses several different computer applications in its daily operations. This audit concentrated on the Adult Correctional Information System (ACIS), which is a set of computer programs designed to track prison inmates, parolees and probationers from the time the offender is convicted to the termination of the sentence. The database holds information regarding such things as criminal convictions, court orders, sentencing conditions, violations and present location.

A discussion of the audit scope and objectives is included in Chapter I. Further detail for the audit issues summarized below is included in Chapters II and III of the report. ***Overall, we concluded general and application controls do not provide for controlled application processing for ACIS.***

Adult Correctional Information System

ACIS is designed to build and maintain consistent and accurate computerized files on offenders. ACIS information assists Probation and Parole (P&P) officers in locating and tracking offenders. Although there is not a direct interface, some of the ACIS information is shared with the state or federal justice systems, as well as the courts. Law enforcement officers use the ACIS database, via telephone requests, to gather information on persons in their custody. Personal information, such as name, mailing address, scars, AKAs, personal description, relationships, etc. are also available on the system.

Information on the System Not Up-to-Date and Complete

We reviewed files of inmates at Montana State Prison (MSP) and offenders under P&P supervision and compared the information in the files to the information on ACIS. Some of the errors found in ACIS records at MSP are: criminal convictions in the offenders files that are not recorded in ACIS, incorrect dates of birth, and a sentence term with a suspended sentence entered incorrectly.

In our comparison of P&P files to the computerized records of offenders, some of the errors we found are: incorrect offender descriptive information, incorrect offense dates, incorrect probation and parole conditions, and a wrong offense code in ACIS for the crime committed. In addition, input of the information is backlogged by about four to six weeks.

Report Summary

Inaccurate Reports

The ACIS system has a reporting function, with several "canned" reports for frequently-requested information. We reviewed several of the reports, and found inaccurate information regarding custody levels of inmates, number of inmates at MSP, number of women inmates at WCC, the next review date for inmate classification, and the total violent and sex offenders in the state. Inaccurate or misleading reports could result in incorrect management decisions or misleading statistics.

Updating of System Tables

A method for ensuring accurate entry of data on the system is through tables. Tables contain lists of valid values or parameters for particular fields. When an entry is made to the fields, the system automatically checks the tables to ensure it is a valid entry. We reviewed the ACIS Offense Code table which contains a listing of offense codes, as defined by state statutes (MCAs), and their descriptions. We found several instances where the information on the table was incorrect or outdated.

Dual "AO" Numbers for Offenders

When offenders become the responsibility of the Department of Corrections through admission to prison or probation, they are assigned a five-digit number unique to them, with an "A0" prefix. For instance, a person may be assigned a number of A012345. That number is to be used only once and is unique to that person. If offenders commit subsequent offenses, that information is added to the existing file, under their original A0 numbers. Thus there should be a central file that contains the entire history of an offender's commitments and offenses. In our testing, we identified instances where individuals were assigned more than one A0 number. If another A0 number is issued to the person, prior offenses and history may be overlooked by corrections personnel dealing with that offender.

Inefficient Functions on the System

During our audit, we noted inefficiencies caused by differences in keyboard layouts at the different offices, inconsistencies of commands used between the screens to perform the common functions, and an on-line help function not being fully utilized.

Documentation

We reviewed the system and user documentation in relation to the ACIS application, and determined there is very limited documentation. Programming and methodology is known by the ACIS programmers, but in the event of their absence there is not adequate documentation to aid in the operation and maintenance of the system.

Electronic Access Controls

Proper access controls prevent and/or detect deliberate or accidental changes caused by improper use or unauthorized manipulation of data, programs, and/or computer resources.

Programmer Access to Production Programs and Data Should be Restricted

DOC programmers have unrestricted and unlogged access to the ACIS production programs and data. This access allows programmers the ability to change any information on ACIS, such as offender sentences and custody levels, without authorization or detection. Programmer activities should be restricted to test programs and files, and all program changes should be tested and approved by the user before they are moved to production.

Segregation of Security and Programming Functions

Industry guidelines recommend that the high level of system authority allowed with the security officer position should be limited to no more than two individuals and duties performed should be independent of programming. Three information services employees have security officer authority.

User Access Should Agree to Job Needs

We reviewed access privileges for ACIS users, and identified several employees with change authority to ACIS who don't need that access to perform their jobs. Some employees at MSP had "command line" authority, which allows them access to inappropriate programs and files on the system.

Password Security Should be Improved

A logon ID, unique to a specific computer user and protected by a password known only to that user, provides a means of limiting access to appropriate users and helps provide accountability for work done. System values are set to require the length of passwords used, how often passwords must be changed, and the content of characters used to form a password. We identified several system values which did not agree with the vendor's suggested values or the state standards for passwords. In addition, two programmers with security

officer authority chose to override the system value that requires their passwords to be changed periodically.

Internal Security Policies and Evaluations

The department does not maintain detailed policies and procedures or perform internal evaluations of security in accordance with state law. Documented security policies, and periodic internal security evaluations could aid the department in maintaining consistent levels of security over the ACIS application and the AS/400 computer system. The electronic access control issues discussed earlier may have been prevented if the department had formal policies and procedures for internal evaluations of security.

Documentation of System and Application Changes

Application Changes - System development and documentation controls should ensure effective security controls are included in all new systems and should preserve the integrity of those controls after the system has been implemented. These controls provide for system documentation, review and testing, and management approval. The department's Information Service Bureau provides programming services to modify or enhance ACIS. However, the department does not have formal procedures to ensure all changes to ACIS programming are properly tested and authorized before being implemented.

Operating System Changes - The Operating System provides overall management and control over applications on the computer. Operating System software should be subjected to the same control procedures as those applied to changes in application programs. The department does not have formal policies or procedures in place for maintaining documentation of changes made to the AS/400 operating system software.

Physical Security Controls

Physical security controls can provide protection over assets, prevent the accidental or intentional destruction of data, and provide for both the replacement of records that may be destroyed and the continuity of operations following a major hardware or software failure.

Environmental Controls

Overall, we found controls are in place to protect the computer system from environmental hazards. Although they maintain fire suppression equipment in the computer room, the department has not installed a smoke detector or a device to detect excessive temperature conditions.

Disaster Recovery Plans Should be Completed

The department has not completed a formal disaster recovery plan to return department applications to normal operations following a disaster.

The department has tested recovery of its AS/400 data center and ACIS in conjunction with tests at the Department of Administration (DofA) hotsite facility. We encourage the department to continue working with DofA to complete disaster recovery procedures for mission-critical applications.

Off-site Storage of Backup Data

Industry guidelines suggest management store backup copies of system software and application programs and data at a secure off-site location to prevent accidental loss. We found that data is being backed up regularly, but is not being stored at a secured off-site storage facility.

Chapter I - Introduction and Background

Introduction

The Department of Corrections (DOC) uses several different computer applications in its daily operations. This audit concentrated on the Adult Correctional Information System (ACIS), which is a set of computer programs designed to track prison inmates, parolees and probationers from the time the offender is convicted to the termination of the sentence. The database holds information regarding such things as criminal convictions, court orders, sentencing conditions, violations and present location. ACIS was designed to build accurate computerized files on offenders to provide information for use by management, probation and parole officers, Board of Pardons, employees at secure facilities, the public, victims, law enforcement and the courts.

This is an electronic data processing audit of general and application controls at the department. We reviewed general controls over the department's AS/400 computer as it relates to ACIS. We also evaluated application controls over ACIS. A review of the application documentation and audit trail was also performed.

EDP Audit General and Application Controls

EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed.

A general control review provides information about the environment in which the computer systems operate and includes an examination of controls in place over the computer applications. Applications must operate within the general control environment in order for any reliance to be placed on them.

Application controls are specific to a given computer application (a set of programs that accomplish a specific function). The review includes an examination of controls over input, processing and output.

Chapter I - Introduction and Background

Audit Conclusions

As discussed in Chapter III of this report, we found several areas where general controls could be improved. Application controls are discussed in Chapter II. We found several areas where input and output controls over the ACIS application could be improved. ***Overall, we concluded general and application controls do not provide for controlled application processing for ACIS.***

Audit Objectives

The objectives of this audit were to evaluate:

1. General controls specific to the department's data processing center which processes ACIS application data. We reviewed the department's data processing center operations and procedures which support ACIS application functions.

2. The effectiveness of application controls over data stored and distributed through ACIS.

Audit Scope and Methodology

The audit was conducted in accordance with government audit standards. We compared the department's general and application controls against criteria established by the American Institute of Certified Public Accountants (AICPA), United States General Accounting Office (GAO), and the information technology industry.

We reviewed the department's general controls related to the computer environment. We interviewed department personnel to gain an understanding of their hardware and software environment, and examined documentation to supplement and confirm information obtained through interviews.

We also reviewed the department's application controls in relation to ACIS. During the planning process, we determined ACIS is primarily a historical database, with minimal processing done by the system. Therefore, we focused our testing of application controls on input and output controls. We reviewed input controls such as input authorization, edits, access controls, and error correction procedures. Also, we reviewed output controls by evaluating the accuracy and validity of data on system generated reports.

In addition, we determined if supporting documentation existed in regard to the ACIS program application, outlining such things as

problem definitions, systems, programs, operations, and user involvement. In addition, we reviewed the department's processes and procedures for use of the ACIS application in tracking all Montana inmates, parolees, and probationers.

Compliance

We determined compliance with state laws and regulations applicable to the ACIS system. We also reviewed the department's compliance with existing department data processing procedures and policy. In addition, we reviewed electronic access controls which ensure department compliance with policies restricting unauthorized access to ACIS information.

Background

The following paragraphs describe the organization of the department at the end of fiscal year 1996-97.

Administrative and support services consists of the Director's Office, the Professional Services Division and the Administrative Services Division. The Administrative Services Division provides personnel, research, facility management, contract, budget, and information services. The Professional Services Division includes legal services, policy coordination, investigative services, department-wide training, inmate classification, health policy coordination, and juvenile detention center licensing activities.

The Board of Pardons, which is attached to the department for administrative purposes only, oversees Montana's inmate parole and furlough programs. The Board also reviews requests for executive clemency and makes recommendations to the governor concerning those requests.

The Community Corrections Division provides supervision and alternative programs for offenders. This division includes Montana Youth Alternatives, Swan River Correctional Training Center, Interstate Compact, Juvenile Placement Unit, Probation and Parole Bureau, Transition Centers, and privatized pre-release centers.

Secure Care Facilities include the Montana State Prison, Women's Correctional Center, and Pine Hills School.

- Montana State Prison at Deer Lodge provides facilities for the custody, treatment, training and rehabilitation of adult male criminal offenders.

- The Women's Correctional Center, previously located on the Montana State Hospital campus, was relocated to Billings in September 1994. The women's system provides facilities for the custody, treatment, training and rehabilitation of adult female criminal offenders.

- Pine Hills School at Miles City provides facilities for the custody, treatment, training and rehabilitation of male youth criminal offenders.

Corrections Enterprises consists of three distinct programs: the Prison Ranch, Industries/Training and the Industries Complex.

- The ranch provides dairy products to state institutions and beef cattle, barley, and surplus milk to the open market.

- The Industries/Training program provides equipment and vehicle repair to state agencies, and meat and vegetable products to state agencies.

- The Industries Complex provides manufactured products (furniture, upholstery, print, signs, sewn goods, license plates, fencing, logs, and firewood) to state agencies, local governments and a retail dealer network.

Chapter II - Adult Correctional Information System

Introduction

The Department of Correction's Adult Correctional Information System (ACIS) is a set of computer programs and user procedures that help track prison inmates, parolees and probationers. The database holds information regarding criminal prosecution, court orders, sentencing conditions, violations, present status, etc. It maintains previous, current and future information on offenders.

ACIS is designed to build and maintain consistent and accurate computerized files on offenders. Decisions regarding parole, probation, good-time, and offender status (dangerous, non-dangerous, etc.) may be made, based in part, on information on the system. ACIS information assists Probation and Parole (P&P) officers in locating and tracking offenders. Although there is not a direct interface, some of the ACIS information is shared with the state or federal justice systems, as well as the courts. Law enforcement officers use the ACIS database, via telephone requests, to gather information on persons in their custody. Personal information, such as name, mailing address, scars, AKAs, personal description, relationships, etc. are also available on the system.

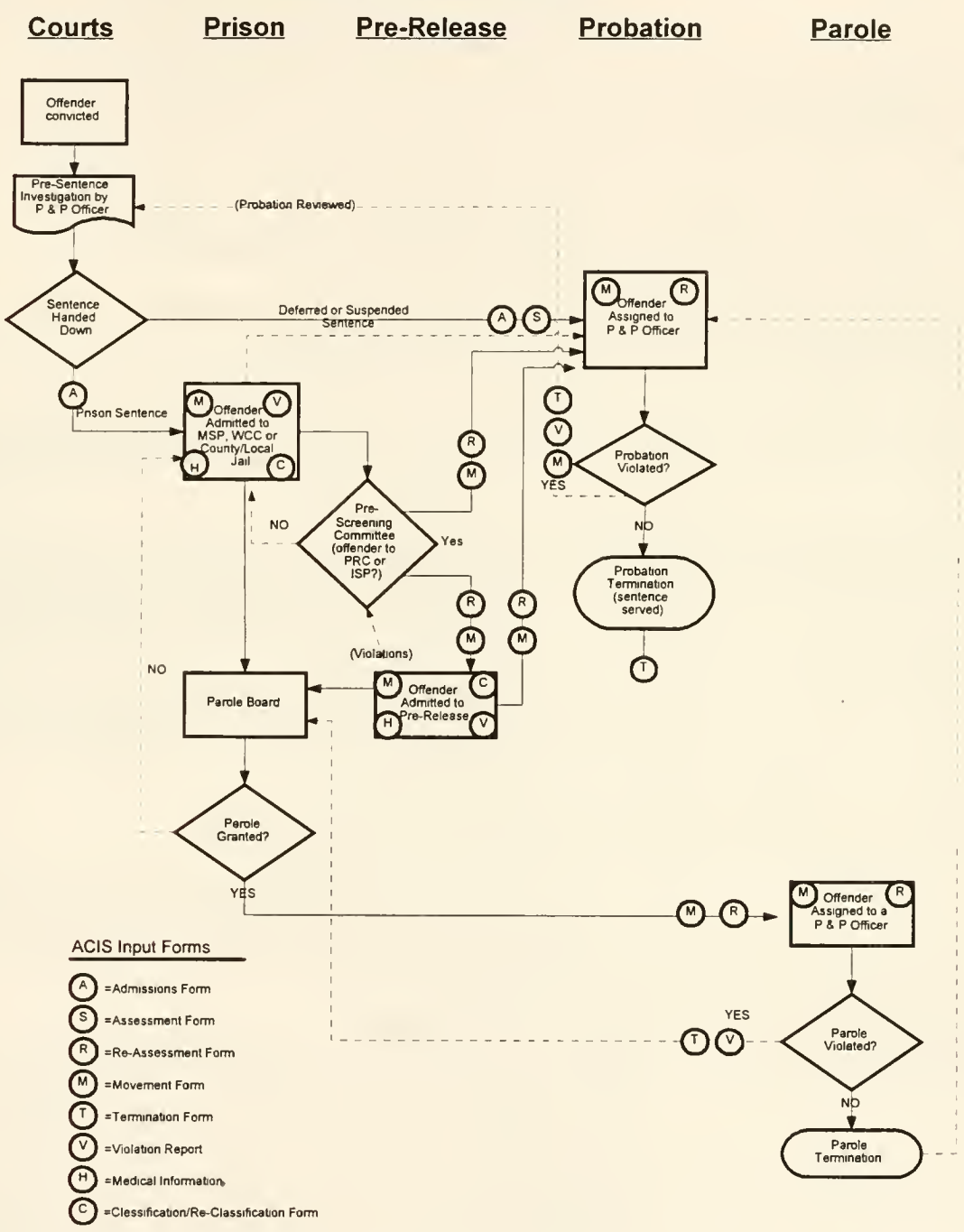
The primary objective of ACIS is to assist the department in tracking the offender's movement within the system, and classification of the offenders. In order to do so, the database must be uniform and accurate. A sound database will enable the department to produce accurate, detailed reports and statistical information pertaining to the movement and classification of all probationers, parolees and inmates.

ACIS operates on the Department of Correction's AS/400 midrange computer, located in the Department of Corrections building in Helena. Information is collected by P&P or prison personnel and is manually entered on forms and input by staff at the central office in Helena, or the administrative staff at the prison. At the time of the audit, only one P&P officer had access to do inquiries on the system. However, by the summer or fall of 1997, the department plans to give all of the P&P officers access to the ACIS system. Until then, any requests for information by P&P staff must be requested through a standard form, or through a phone call to the central office.

The following figure shows the general movements an offender can make through the corrections system, and the forms required at each stage. The information on the forms should also be input to ACIS.

Figure 1

CORRECTIONS SYSTEM--OFFENDER ASSIGNMENT/FLOW



Source: Compiled by the Legislative Audit Division

Information on the System Not Up-to-Date and Complete

We reviewed files of 47 current inmates at Montana State Prison (MSP) and 44 offenders under P&P supervision and compared the information in the files to the information on ACIS. We did not test the accuracy of the information in the files. We only tested whether the information in the files was accurately input to ACIS.

Montana State Prison Testing

Following is a summary of errors found at MSP:

- Two incorrect dates of birth.
- One incorrect Social Security Number (SSN).
- One case where scars and marks were input incorrectly, and one where they were not input at all.
- One incorrect court docket number.
- Four offenses that were in the files, but had not been input to ACIS, including:
  - -- Offense of theft, with a prison sentence of eight years;
  - -- Offense of deliberate homicide, with a prison sentence of two life terms (ACIS showed the offender with only one count of theft, one count of issuing a bad check, and one count of bail-jumping);
  - -- Offense of felony assault, with a one year prison sentence;
  - -- Offense of sexual intercourse without consent--25 years, with 5 years suspended.
- One offense date entered incorrectly.
- One sentence of two 20-year terms with eight years suspended on each was recorded on ACIS as one 20-year sentence with 20 years suspended (suspended sentence later revoked, due to probation violation).

Inmate Classification Not Input to ACIS

We also reviewed classification information for the inmates. Classifications and reclassifications are required for all inmates at least every six months. The classifications are done by unit supervisors, and determine the custody level required for the inmate. The inmate may be classified as "maximum" (highest security risk), "close," "medium restricted," "medium unrestricted," "minimum restricted," or "minimum unrestricted" custody level. The custody level

determines which prison unit the inmate will be housed in, and the level of supervision that will be required. A reclassification may or may not change the inmate's custody level.

For sample items tested, we found many of the classifications were not being input to ACIS. MSP personnel stated if the prisoner's custody level had not changed since the last reclassification, the information was often not updated to ACIS. However, part of the information input from the reclassification form is the "next review" date. ACIS produces a report titled "Date of Next Review," which gives a listing of inmates due for reclassification in a given time period and keys on the "next review" date. Since the reclassification information is not kept up-to-date on the system, that report is not accurate and cannot be relied upon as a useful management tool.

Probation & Parole Office Testing

We also reviewed 42 sample items at two district P&P offices. Following is a summary of our findings:

- In eight cases, descriptive information was input incorrectly (name, date of birth, height, scars, marks, descriptions).
- Four cases where the court docket number was missing or incorrect.
- Six cases with incorrect offense date.
- Two cases with incorrect sentencing judge.
- Eight cases where special conditions were incomplete or incorrect.
- One case where the offense code was entered incorrectly.
- One case where the personal ID number for the offender on ACIS is different than what is in the files.

Assessments Not Updated and Input to ACIS

Offenders on probation or parole are assessed periodically to determine what level of supervision is required. Frequency of assessments varies depending on their current level of supervision. For instance, a person assessed as "maximum" or "extended" supervision is required to be re-assessed at least every six months, while a person on "minimum" or "admin" needs to be re-assessed only when new information is received which may affect supervision level. In our sample testing, we found two cases where the assessments were not done within the required time period. In addition, in seven cases the assessments were not input to ACIS and in one case the recorded assessment was incorrect.

Data Input is Backlogged

Most of the P&P information is input at the Helena office, from forms supplied by the P&P officers. On average, input of the information is backlogged by about four to six weeks.

If the ACIS system is used in decision-making by the prison staff and the P&P officers, inaccurate or incomplete information on the system could result in repeat offenders not being properly identified, skewed statistical and management reports, delayed classifications and assessments, or undue delay of processing an offender because the necessary information is not available. This will be especially critical pending the addition of all P&P officers who will have direct access to the ACIS information.

Given the critical nature of the information contained on ACIS, the agency should take steps to ensure the information is correct, complete, and useful. The department should consider:

1. Implementing a double-check or verification procedure, to ensure information is accurately input to ACIS.

2. Ensuring all assessments and classifications are being done as scheduled and are being updated to ACIS.

3. Assigning additional staff for the input of data to ACIS to ensure the information on ACIS is current.

Recommendation #1

We recommend the department ensure accuracy and completeness of information on the ACIS system.

Inaccurate Reports

The ACIS system has a reporting function with several "canned" reports for frequently-requested information. We reviewed several of the reports to determine if the information they provide is accurate and complete. Following is a summary of errors or inaccuracies found in various reports.

Custody Levels - This report gives a count of all inmates in the prison and their custody level, as of a designated point in time. We found there are some inmates with no custody level recorded on ACIS (classification information was never input). In those cases, the inmates were not counted in the report. We determined there were 21 inmates at MSP and 20 inmates at WCC that were not being reported on this report, as of 2/14/97.

In addition, when inmates are admitted to MSP, they are initially housed in a cell-block called "reception." While in reception, they are automatically classified as CLOSE custody, until they are officially classified and moved to another cell-block. However, on the custody level report there is no distinction between a "classification decision" and the default classification for inmates in reception. Therefore, this report may indicate an inordinate number of CLOSE custody inmates, since many of those inmates in reception may actually be at maximum, medium, or minimum security, once a classification decision is made.

Alpha Listing of Current MSP Inmates - Although the title suggests it is a report of only current MSP inmates, it includes all males under the supervision of the Department of Corrections, including inmates residing in the Texas facility, pre-release residents, Boot Camp residents, and parole violators. In addition, we found 25 current inmates who were not included in the report.

Alpha Listing of Current WCC Inmates - We noted the same problems as the MSP report. In addition, we noted a male inmate on the WCC report. This person was input in ACIS as "F" in the sex field. Therefore, he is picked up in the WCC report, but not in the MSP report. We verified he is actually residing in MSP. However

several other reports, including the ones noted above, will be incorrect because of this error.

Violent Offenders by County - We found there are many duplicates in this report. In some cases, the offender appears six or more times in the report. We also found several cases where violent offenders on the system do not appear on the report. In addition, out of state or juvenile offenders who are required to register, but have not spent time in the Montana system, are never entered to ACIS and do not show up on the report. Therefore, since the report counts some offenders more than once, and doesn't count others at all, it is not a reliable source of information.

Sex Offenders by County - There are many duplicates in this report also. In some cases, the offender appears six or more times in the report. We also found several cases where sex offenders on the system do not appear on the report. In addition, out of state or juvenile offenders who are required to register, but have not spent time in the Montana system, are never entered to ACIS and do not show up on the report. Therefore, since the report counts some sex offenders more than once, and doesn't count others at all, it is not a reliable source of information.

Next Review Reports - This report gives the date an inmate is due for his next reclassification of custody level. We found several cases where a next review date was either not available (blank), or was not updated after the most recent reclassification (see discussion on page 8). Since the report picks up the field based on a date range (for example, all inmates due for reclassification between March 1, 1997 and March 30, 1997), many scheduled reclassifications will not show up on this report.

Inaccurate or misleading reports could result in incorrect management decisions or misleading statistics. The department should ensure the reports are accurate and complete, and that the titles give accurate descriptions of the contents of the reports.

Recommendation #2

We recommend the department review the present reports and ensure they are compiling the information accurately and completely.

Updating of System Tables

A method for ensuring accurate entry of data on the system is through tables. Tables contain lists of valid values or parameters for particular fields. When an entry is made to the fields, the system automatically checks the tables to ensure it is a valid entry. As the values and parameters change, the user need only make the change on the tables, rather than making changes to the various programs.

We reviewed the ACIS Offense Code table which contains a listing of offense codes, as defined by state statutes (MCAs), and their descriptions. The offense codes on the table should be numbered to match the MCA numbers. However, we found several instances where the information on the table was incorrect or outdated. For instance, there were some offense codes that showed a different offense than the MCA of the same number. Other offense codes were still active on the table, although they had been repealed in the MCAs. Several offenses were listed on the table more than once, under different offense numbers.

Since the offenses are entered onto ACIS based on the MCA number, inaccurate information on the table could result in incorrect offense descriptions on the system. Also, for statistical purposes, offenses may be listed under two or more offense codes. Therefore some of the offenses may not be included in the program search for the selected type of offense.

We interviewed department personnel and reviewed documentation to determine who is responsible for maintaining the tables and ensuring they are accurate and up-to-date. Information Services Bureau (ISB) personnel are responsible for making changes to the tables, as requested. However, we found that no one person or group is responsible for ensuring the tables are accurate and up-to-date. The department should review the tables and inactivate any offense codes that no longer apply. Also, they should compare the offenses with the MCAs, to ensure all of the codes are current and the descriptions are accurate.

Recommendation #3

We recommend the department assign responsibility to:

A. Review the offense code table, and inactivate any codes that no longer apply.

B. Periodically compare the table to the MCAs and ensure the table codes agree with the MCA codes.

Dual "A0" Numbers for Offenders

When offenders become the responsibility of the Department of Corrections through admission to prison or probation, they are assigned a five-digit number unique to them, with an "A0" prefix. For instance, a person may be assigned a number of A012345. That number is used only once and is unique to that person. If offenders commit subsequent offenses, that information is added to the existing file, under their original A0 numbers. Thus there should be a central file that contains the entire history of an offender's commitments and offenses.

For assigning the A0 numbers, the AS/400 has a numbering facility referred to as the "phone file." This file contains a listing of all A0 numbers issued, along with the name and date of birth of the person to whom it is assigned. An employee performs a search of the phone file by last name and/or date of birth, to determine if the person is already on the system. If a match is not found, the next unused A0 number in the sequence is assigned to that person.

In our testing, we identified instances where individuals were assigned more than one A0 number. This seemed to occur because of incomplete searches for matches. On ACIS, there is also a function to allow searches against SSN and AKAs. However, this function is not available to the help desk personnel. If another A0 number is issued to the person, prior offenses and history may be overlooked by corrections personnel dealing with that offender.

In order to ensure records are centralized and complete, the department should review the present records for duplicates. In addition,

the department should fully utilize the search functions available to ensure additional records are not created for existing offenders.

Recommendation #4

We recommend the department ensure each offender has only one complete record on the ACIS system.

Inefficient Functions on the System

During our audit, we noted the following inefficiencies:

- Keyboard layout varies between computers used in the Helena office and computers used in the MSP and P&P Offices. Consequently, there are different sequences of keys to be pushed to get the commands to work properly depending on the location of the office in which employees are working.

- There is an inconsistent setup of the commands used between the screens within a computer. Experienced users of ACIS in the department complained of difficulties moving around in the system. For example, while working in different areas of one file, different function keys are required to exit screens. In some screens, selecting the common command will exit the user from the ACIS system completely, requiring the user to reenter the ID and password to return to the system.

  On several of the screens, there is an "options" bar at the bottom of the screen, which often gives the user incorrect instructions on how to move from screen to screen or access additional data. For instance, on some screens the user is instructed to use F7 and F8 to page up or down, but the actual commands may be "page up" "page down" "enter" or the arrow keys, depending on the individual screen.

- An on-line help function is often indicated as an option on the screens, to assist the user in data entry, and movement on the system. In some cases, the help is available, but in most cases the help function was disabled or blank.

If the system is not easy to use and understand, users may get frustrated and decide not to enter some information to the ACIS system. In addition, it may take longer to input the information than would

otherwise be required. The department should re-design the ACIS input/inquiry screens to make them more easily understandable by the users.

Recommendation #5

We recommend the department review the ACIS computer screens, and improve the accuracy of on-line instructions and consistency between screens, to make the system easier to use and understand.

Documentation

Good documentation is important to the design and implementation of a well-controlled system and serves as a source of information in the study and evaluation of accounting control. EDP documentation defines the system and procedures for performing data-processing tasks. Documentation generally provides:

1. An understanding of a system's objectives, concepts, and output.
2. A source of information for systems analysts and programmers who are responsible for maintaining and revising existing systems and programs.
3. Information necessary for supervisory review.
4. A basis for training new personnel.
5. A means of communicating common information to other system analysts, programmers, and operators.
6. A source of information about accounting controls.
7. A source of information needed to provide continuity in the event of loss of experienced personnel.

We reviewed the system and user documentation in relation to the ACIS application, and determined there is very limited documentation. Programming and methodology is known by the ACIS programmers, but in the event of their absence there is not adequate

documentation to aid in the operation and maintenance of the system.

As noted in other sections of this report, there are also other areas where documentation is either incomplete or non-existent. These areas include: approval, testing and authorization of system and application development and changes; policies and procedures regarding ACIS access; disaster recovery policies, procedures, and testing; internal security policies; and table review policies and procedures.

The department should ensure the critical operations of the ACIS system are documented, to ensure continuity of operations in the event of employee turnover, or damage to computer equipment or software.

Recommendation #6

We recommend the department maintain up-to-date documentation of all critical processes and policies for the operation of the ACIS system.

Chapter III - General Controls

Introduction

The department's Information Services Bureau (ISB) operates the AS/400 computer processing center, located in the Corrections building in Helena. ISB provides programming and maintenance to support computing and information requirements for the department. ACIS is one of seven applications run on the AS/400; three applications are used for Department of Corrections (DOC), and the other four applications belong to Department of Public Health and Human Services (DPHHS). In our review of general controls over the mainframe computer environment in relation to Adult Correctional Information System (ACIS) we found weaknesses in organizational, hardware and system software, physical security, data and procedural, electronic access and system development controls. We discuss these issues in the following sections.

Electronic Access Controls

Access controls provide electronic safeguards designed to protect computer system resources. Logon IDs and passwords control access to ACIS computer programs and data. Access is also controlled by the level of "authority" granted to a user; system authorities may be assigned which allow a user to perform various functions, such as changing or adding programs, adding or deleting other users on the system, or adding or deleting data in a file.

Proper access controls prevent and/or detect deliberate or accidental changes caused by improper use or unauthorized manipulation of data, programs, and/or computer resources. The department's security officer is responsible for insuring all production files are protected, access authorizations are properly documented, and user access is limited to specific ACIS application areas where appropriate. Assigning limited access based on job duties prevents users from inadvertently or willfully executing programs, and/or changing data unrelated to their job.

Programmer Access to Production Programs and Data Should be Restricted

Four DOC programmers have unrestricted and unlogged access to the ACIS production programs and data. Industry standards suggest management prohibit programmer access to production programs and data. In addition, industry standards state ". . .that no one person has incomplete duties that would permit the perpetration and concealment of material errors or irregularities." The present access allows programmers the ability to change any information on ACIS, such as offender sentences and custody levels, without authorization or detection.

Because of their high degree of technical knowledge, programmers should not have access to the production programs or files. Their activities should be restricted to test programs and files, and all program changes should be tested and approved by the user before they are moved into production.

ISB programmers indicated they need unrestricted access to aid in user support. They noted errors often occur during production data processing and require programmers to resolve the error. We believe DOC should limit programmer access to production programs and data. When user support is required, access to production programs could be enabled temporarily, then disabled once the problem is fixed. All access by the programmers should be logged and changes should be reviewed by management.

The AS/400 computer system provides a logging function which DOC currently does not use. Using this function, all activity within a specified file or program could be recorded for review by management. DOC personnel indicated enabling the logging function requires considerable data storage space. The department's AS/400 is operating close to full capacity, and as a result, prevents DOC from enabling the logging function. Part of the reason the AS/400 is operating close to full capacity is that four applications belonging to DPHHS are occupying a large amount of available space. Custody of these applications transferred from DOC to DPHHS after the reorganization in 1995. The department could remove DPHHS applications from the AS/400 to allow for more efficient and effective operation of its own applications.

Programmer access to production programs and data should be restricted. At a minimum, we believe DOC should log all programmer access to the application production programs and files, and the ISB bureau chief should review the log periodically.

Recommendation #7

We recommend the department implement controls to limit programmer access to production programs and data.

Segregation of Security and Programming Functions

The department security officer is responsible for maintaining secure system operations, granting users appropriate access, and insuring all production files are protected. Industry guidelines recommend that the high level of system authority allowed with this position should be limited to no more than two individuals and duties performed should be independent of programming. Three employees in ISB have security officer authority. Two of the three employees are also responsible for AS/400 system and ACIS programming, and the other stated he does not perform security functions, and therefore, does not need the access.

As discussed in the previous section, programmer access to production programs and data should be restricted. Since security access allows unlimited access to all programs and files on the system, someone other than the programmer should be assigned the security officer function.

Department personnel stated because of the small size of ISB, they are unable to separate the duties of the security officer, AS/400 system programming, and ACIS programming. However, someone outside of ISB could perform the duties of security officer. In addition, because of the high level of access granted to the security officer, all changes made with the security officer profile should be logged and reviewed by management.

Recommendation #8

We recommend the department:

A. Assign the security officer function to someone other than programmers.

B. Log and independently review all changes made with the security officer ID.

User Access Should Agree to Job Needs

ACIS users include employees at the central office in Helena, Montana State Prison, Women's Correctional Center, and probation and parole officers throughout the state. The department assigns employee access to ACIS information based on an employee authorization form that specifies which functions will be performed. Each division supervisor is responsible for approving access changes and notifying ISB of terminated employees. The approved authorization form is then sent to ISB for implementation by the department security officer.

We reviewed access privileges for all ACIS users. The objective of our testing was to determine if personnel with write access to ACIS need it to perform their jobs. Of 112 users tested, we identified 20 with change authority to ACIS who do not need that access to perform their jobs. Fifteen of these employees had either changed positions within the department and no longer needed the same level of access, or had terminated employment with DOC. However, the department security officer had not been notified of the changes. Five employees at MSP (including one mail room clerk and four office employees) had "command line" authority, which allows them inappropriate access to programs and files on the system. This access was inadvertently given to those employees over a period of several years without detection. In addition, 12 employees had not used their IDs to access ACIS for at least seven months. For one of these IDs, the system had logged 402 invalid sign-on attempts which the department was unable to locate and resolve.

Unauthorized or unnecessary write access to ACIS exposes the system to accidental or intentional changes and deletions. Management should limit ACIS access to those users needing it in the performance of their duties. For example, they could require department supervisors to review current employees' access levels to determine if access needs have changed, and are reasonable. In order to be effective, these access reviews should be performed every six months to a year.

Recommendation #9

We recommend the department:

A. Review current computer system access levels and remove access from those not needing it to perform their jobs.

B. Develop procedures for periodic review of access levels for reasonableness.

Password Security Should be Improved

A logon ID, unique to a specific computer user and protected by a password known only to that user, provides a good means of limiting access to appropriate users and helps provide accountability for work done. Security-related system values are assigned and adjusted to tailor the security for the department's AS/400. Values are set to require the length of passwords used, how often passwords need to be changed, and the content of characters used to form a password. We identified several system values which did not agree with the vendor's suggested values or the state standards for passwords. For instance, state standards require changing of passwords every sixty days, and a minimum password length of six characters. The department's system values were set at ninety days for changing of passwords, and a minimum length of five characters.

In addition, two programmers with security officer authority chose to override the system value that requires their passwords to be changed periodically. The first programmer's two passwords had not been changed since 4/30/93 and 12/20/94, and the second programmer's password was last changed on 2/28/96. The

programmers changed the value so they wouldn't need to remember as many passwords. These programmers have the highest level of authority on the system, which causes it to be even more critical that their passwords comply with security policies. The department agreed to change the password values to require programmers to create new passwords every 60 days.

Industry guidelines suggest management implement available safeguards to prevent unauthorized system access. The overall security over access is reduced when system values are more lenient than the required and suggested values.

Recommendation #10

We recommend the department ensure password procedures are in compliance with state policy.

Internal Security Policies and Evaluations

The department does not maintain detailed policies and procedures or perform internal evaluations of security in accordance with state law. Section 2-15-114, MCA, requires department heads to be ". . . responsible for assuring an adequate level of security for all data and information technology resources within his department and shall . . . (1) develop and maintain written internal policies and procedures to assure security of data and information technology resources . . . (4) ensure internal evaluations of the security program for data and information technology resources are conducted. . . ."

The department should establish policies and procedures in accordance with state law which address safeguarding data and information technology resources including microcomputer policies and program documentation. As defined in state policy (MOM 1-0250.00), these procedures include, but are not limited to, the following:

1. Develop and maintain written internal policies and procedures to assure security of data and information technology resources.

2. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data and information technology resources.

3. Ensure that periodic internal evaluations of the security program for data and information technology resources are conducted.

Documented security policies, and periodic internal security evaluations could aid the department in maintaining consistent levels of security over the ACIS application and the AS/400 computer system. The electronic access control issues discussed on pages 19-24 may have been prevented if the department had formal policies and procedures for internal evaluations of security.

Recommendation #11

We recommend the department:

A. Expand current internal policies and procedures to assure security of data and information technology resources.

B. Ensure internal evaluations of the security program for data and information technology resources are conducted in accordance with state policy (MOM 1-0250.00).

Documentation of System and Application Changes

Application Changes - System development and documentation controls should ensure effective security controls are included in all new systems and should preserve the integrity of those controls after the system has been implemented. These controls provide for system documentation, review and testing, and management approval. The department's ISB provides programming services to modify or enhance ACIS. However, the department does not have formal procedures to ensure all changes to ACIS programming are properly tested and authorized before being implemented.

Authorization and testing of changes are often done informally, and documentation of the changes and subsequent testing is not maintained. Consequently, changes have been made to the application,

with little or no evidence as to who performed the change, whether the change was tested, and who requested/approved the change. For instance, as discussed on pages 11 and 12, several reporting programs were produced and added to the ACIS reports menu that were either inaccurate or misleading.

Industry standards suggest management establish procedures to ensure all changes to a system are approved before implementation to determine whether they have been authorized, tested, and documented. Documentation provides a source of information for systems analysts and programmers who are responsible for maintaining and revising existing systems and programs; a basis for training new programming personnel; and a source of information needed to provide continuity in the event of loss of experienced personnel.

Recommendation #12

We recommend the department develop formal procedures for requesting, authorizing, testing, and documenting all changes to the ACIS application.

Operating System Changes - The Operating System provides overall management and control over applications on the computer. Operating System software should be subjected to the same control procedures as those applied to changes in application programs. The department does not have formal policies or procedures in place for maintaining documentation of changes made to the AS/400 operating system software.

Industry standards suggest that documentation be maintained of the authorizing, testing, and approval of all changes made to systems software. Documentation would help provide for continuity in the event of loss of experienced personnel. Department personnel stated they have not documented system changes because of the small size of the computer operations center and the infrequency of system changes.

The department should develop procedures to ensure changes to the operating system are properly authorized, tested and approved before being implemented. In addition, they should maintain documentation of the changes and related testing.

Recommendation #13

We recommend the department develop formal procedures for requesting, authorizing, testing, and documenting all changes to the operating system software.

Physical Security Controls

Physical security controls can improve the protection over assets, prevent the accidental or intentional destruction of data, and provide for both the replacement of records that may be destroyed and the continuity of operations following a major hardware or software failure. Physical security controls include: safeguarding of files, programs and documentation; physical safeguarding of the computer facility; and a plan or method to ensure continuity of operations following major destruction of files, or hardware breakdown.

Environmental Controls

We reviewed existing environmental controls within the data center. Overall, we found controls are in place to protect the computer system from environmental hazards. The department restricts access to the facility to authorized personnel, and maintains a backup power supply in the event of power outages. Although they maintain fire suppression equipment in the computer room, the department has not installed a smoke detector or a device to detect excessive temperature conditions. Electronic devices can be installed to provide 24 hour surveillance which places an emergency telephone call to notify personnel of potentially damaging conditions, such as fire or air conditioner failure.

Industry standards suggest management implement controls to prevent or limit damage to computer equipment caused by excessive heat or fire. Because the computer facility is not supervised after-hours and is periodically left unattended throughout the day, a smoke detector and/or monitoring device could alert employees of

fire or extreme temperatures. The cost of this equipment is minimal compared to the potential cost of extensive damage or loss of computer hardware.

Recommendation #14

We recommend the department install fire and temperature detection devices to prevent or limit damage to computer facility equipment.

Disaster Recovery Plans Should be Completed

The department has not completed a formal disaster recovery plan to return department applications to normal operations following a disaster. An effective disaster recovery plan should allow management to restore computing operations in a timely manner, and minimize losses due to computer down-time.

Industry standards suggest management develop formal procedures to efficiently recover computer processing activities to normal operations following a disaster. The Montana Operations Manual section 1-0240.00, outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing information and resource requirements necessary to maintain applications; and determining alternate procedures which may be necessary if recovery is not timely.

A disaster recovery plan may include but is not limited to:

- An inventory of current applications, operating system programs, telecommunications programs or networks, and hardware.
- An analysis to determine application significance and impact of loss, to define mission-critical applications which must be recovered.
- An analysis to determine application recovery priority.

- Selecting a disaster recovery method depending on how long the organization can operate without processing, management's backup procedures, and cost.

- Identification, involvement, and commitment of employees responsible for operating applications.

- Definition of application requirements including personnel, hardware, system support programs, communications, data, special forms, etc.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a complete disaster recovery plan which defines department responsibilities and requirements, the department may be unable to recover its applications in a timely manner.

The department has tested recovery of its AS/400 data center and ACIS in conjunction with tests at the Department of Administration (DofA) hotsite facility. Although DofA can recover agency applications and provide mainframe connection capabilities for agency-owned terminals, it cannot define agency application recovery priorities or personnel responsibilities. We encourage the department to continue working with DofA to complete disaster recovery procedures for mission-critical applications.

Recommendation #15

We recommend the department continue to document and test formal disaster recovery procedures for department mission-critical applications.

Off-site Storage of Backup Data

We reviewed department procedures which ensure AS/400 System and ACIS data are backed up regularly and stored in a secure location to prevent accidental loss. The department performs a monthly backup of the operating system. The tapes are stored at the home of the employee performing the backup. The department has no assurance the tapes are stored in a secure environment. Also, the tapes may not be easily accessible if the employee cannot be contacted.

In addition to the monthly backups, nightly backups of ACIS data are created, and stored in an office next to the computer room. These tapes are available for recovery if the computer "crashes," and the data is lost. However, if there is an event that effects the entire building, such as fire or flood, both the computer and the backup tapes could be damaged and up to one month of data input could be lost. The department could mitigate their losses by storing daily, or even weekly backups at a secured offsite storage facility.

Industry guidelines suggest management store backup copies of system software and application programs and data at a secure off-site location. The Department of Administration provides a secured off-site storage, including pick-up and delivery, for agency backup data.

Recommendation #16

We recommend the department ensure backup information is stored in a secure off-site location.

Agency Response

DEPARTMENT OF CORRECTIONS

MARC RACICOT, GOVERNOR

1539 11TH AVENUE

STATE OF MONTANA

(406) 444-3930
FAX: (406) 444-4920

PO BOX 201301
HELENA, MONTANA 59620-1301

September 5, 1997

RE: Response to Legislative Audit Recommendations
EDP Audit - Adult Correctional Information System

Mr. Scott Seacat
Legislative Auditor
Legislative Audit Division
Capitol Station
Helena, Montana 59620

Dear Mr. Seacat:

Attached is the Department's response to the Legislative Audit Recommendations contained in the EDP Audit of the Adult Correctional Information System (ACIS) completed in July 1997. We hope the response to reflects the continuing cooperative spirit between our agencies and our goal of improving correctional data systems.

Since the Legislative Auditor and Department do not deal with information system audits on a regular basis, some background is presented below.

The ACIS system was designed in 1983 and implemented in 1985 by the then Department of Institutions. Although the corrections facilities were a part of the Department, they had not even been consolidated for accounting purposes at that time. Also, in the 1983 - 1985 period, Montana State Prison and the adult male system were by far the major players in development. Consequently, the system was built to operate for MSP and Probation & Parole. During the 10 year period from 1985 to 1995, the programs and systems were supported and updated by the same staff level while the inmates in the corrections more than doubled.

In 1994-95, an effort was initiated to begin to computerize the department. Personal computers and networks were placed in priority areas. The priority was to allow sharing and transmission of data between all facilities of the then Department of Corrections and Human Services which during this time included Montana State Hospital, the Center for the Aged, Montana Veterans Homes in Columbia Falls and Glendive, and the Alcohol and Drug Abuse program in Butte, as well as community programs in mental health and alcohol and drug abuse.

The department prepared a request for additional Information Services FTE and funding for the 1995 Legislature. The data processing request was not included in final appropriations. Also, that session directed a major reorganization of human services and corrections which resulted in the current Department of Corrections which now has both adult and juvenile corrections components. The 96-97 biennium budget of the Department resulted in a supplemental request for funding which did not allow any current level funding savings to address data processing issues during that period.

In preparation for the 1997 Legislature, the Department analyzed its needs in data processing and prepared a request for funding which would allow (1) placing and up-grading infrastructure for systems in the Department, (2) purchasing new and replacement equipment, (3) planning for attachment of regional prisons to department systems, (4) implementing new technology in finger print and photo identification in the department and in regional prisons which will interface with Department of Justice files, (5) upgrade current data systems through adding accuracy, timeliness and effectiveness and (6) adding new data systems which are needed for analysis of programmatic decisions. The 1997 Legislature funded an automation project of $2.7 million over the biennium which was about 80% of the Department request. The funding was contained in HB2, the regular appropriation bill, and in HB188 (the bonding for automation bill). Additional FTE were included and funded to begin in October, 1997.

Many of the issues outlined in the EDP Audit report were recognized and included in the plans of the Department for implementation of the 1997 appropriation.

The 1997 Legislature instituted a Correctional Standards and Oversight Committee which will be reviewing the operations of the Department during the 1998-99 biennium. The Department will keep the Oversight Committee informed of progress on the automation plan.

Sincerely,

RICK DAY
Director

Attachment

G:\fiscal\audit\auditedp.097

DEPARTMENT OF CORRECTIONS
ADULT CORRECTIONAL INFORMATION SYSTEM (ACIS)
EDP AUDIT RECOMMENDATION RESPONSE
September 5, 1997

Recommendation #1:

We recommend the department ensure accuracy and completeness of information on the ACIS system.

Response:

Concur. As a part of implementation of the legislatively approved corrections information system project, the department has assigned a position responsible for accuracy and completeness of information placed in the data systems developed during the biennium under the information plan and for review of both current and new reports for usefulness and accuracy. Hiring should be complete by December 31, 1997.

Recommendation #2:

We recommend the department review the present reports and ensure they are compiling the information accurately and completely.

Response:

Concur. The reports discussed have been corrected, with two exceptions. First classifying offenders in Reception as CLOSE custody accurately reflects Montana State Prison's policy. It is, therefore, accurate. Second, The Sex and Violent Offenders Reports were designed to "double count" as an offender may commit crimes in more than one county. The Department is currently in the process of transferring the registry to the Department of Justice in compliance with 1997 Legislative action. The transfer to Justice will be effective October 1, 1997.

Recommendation #3:

We recommend the department assign responsibility to:

A. Review the offense code table, and inactivate any codes that no longer apply.

B. Periodically compare the table to the MCAs and ensure the table codes agree with the MCA codes.

Response:

Concur. The offense codes in the system tables which refer to outdated or repealed MCAs will be inactive for new cases but will be required to remain in the system to provide historical accuracy. The data coordinator function referred to in response to recommendation # 1 will have as a portion of the function a review of the code changes required by law or policy change at least on an annual basis. Hiring of the position will be completed by December 31, 1997, and the function will be ongoing from that point. A review of all codes in the current systems will be completed prior to programming under the Automation Plan.

Recommendation #4:

We recommend the department ensure each offender has only one complete record on the ACIS system.

Response:

Concur. Please see response to recommendation #1.

Recommendation #5:

We recommend the department review the ACIS computer screens, and improve the accuracy of on-line instructions and consistency between screens, to make the system easier to use and understand.

Response:

Concur. The department will include in its review and of current systems the input screens and directions to users provided by the system. The updated system will include user friendly screens and appropriate user training will be in place at the completion of the Automation Plan.

Recommendation #6:

We recommend the department maintain up-to-date documentation of all critical processes and policies for the operation of the ACIS system.

Response:

Concur. The department will include documentation requirements in all changes made in systems and processes implemented through the Automation Plan.

Recommendation #7:

We recommend the department implement controls to limit programmer access to production programs and data.

Response:

Concur. The department will be able to come into compliance once the AS/400 upgrade, scheduled for December, 1997, is completed. By April 1, 1998, a partition will be set up and available for programmers to develop and test systems outside of the production environment. All program changes are currently tested by the user before being moved into production.

Recommendation #8:

We recommend the department:

A. Assign the security officer function to someone other than programmers.

B. Log and independently review all changes made with the security officer ID.

Response:

Concur. The department is in the process of realigning staff duties to implement this recommendation. We expect to comply by December 1, 1997.

Recommendation #9:

We recommend the department:

A. Review current computer system access levels and remove access from those not needing it to perform their jobs.

B. Develop procedures for periodic review of access levels for reasonableness.

Response:

Concur. The department was able to locate and resolve the invalid sign-on attempts. Command line authority only allows someone to do what the rights they are granted permit them to do, which they could do anyway without the command line authority. The problems with the 20 people with too much authority and the 12 inactive sign-ons have been fixed. An interim procedure has been put in place which reviews bi-weekly all security levels on the AS/400 and on the DOC Wide Area Network. This recommendation is partially implemented and will be finalized and documented by January 1, 1998.

Recommendation #10:

We recommend the department ensure password procedures are in compliance with state policy.

Response:

Concur. The department has corrected all passwords and they are now in compliance with state policy. This recommendation is implemented and on-going.

Recommendation #11:

We recommend the department:

A. Expand current internal policies and procedures to assure security of data and information technology resources.

B. Ensure internal evaluations of the security program for data and information technology resources are conducted in accordance with state policy (MOM 1-250.00).

Response:

Concur. Discussion leading to Recommendation #11 implies that the Department does not have a security policy. DOC Policy 1.6.7 addresses security issues. Copies were provided to the auditors during the audit. In compliance with the recommendation, the Department will begin a review of the current policy during January, 1998, and request input and clarification from Audit Staff to expand DOC policy.

Recommendation #12:

We recommend the department develop formal procedures for requesting, authorizing, testing, and documenting all changes to the ACIS application.

Response:

Concur. The Department will develop formal written procedures and share a draft for Legislative Auditor comment prior to final adoption projected for February 1998.

Recommendation #14:

We recommend the department install fire and temperature detection devices to prevent or limit damage to computer facility equipment.

Response:

Concur. The department has requested an estimate of cost for installation of smoke detection equipment in the computer facility area from the General Services Division of the Department of Administration. When estimated cost of equipment and installation are known, the department will review current level budgets to determine if the funds can be found during the current biennium or must be requested from the next Legislature. The implementation date of this recommendation will depend upon cost and funding availability.

Recommendation #15:

We recommend the department continue to document and test formal disaster recovery procedures for department mission-critical applications.

Response:

Concur. As noted by the auditor in this report, the department has an on-going working relationship with the Department of Administration and has tested recovery of its AS/400 data center. We will continue to update and refine the disaster recovery plan. This recommendation is implemented and on-going.

Recommendation #16:

We recommend the department ensure backup information is stored in a secure off-site location.

Response:

Concur. Arrangements have been made with the Department of Administration to store all backup tapes in the Information Services Division's Computer Room. Tapes are being transported on a daily basis. This recommendation is implemented and complete.